Bellevue Police Department

ATM Skimming

ATM skimming is a term used to describe the method criminals employ in order to capture the account information on the back of your bank cards when you use ATM's and point of sale terminals. They then use this information to access and remove money from your accounts at a later date.

In a typical ATM skimming scenario, a criminal will locate an ATM machine to target. Once the ATM machine is selected, the criminal will do two things in order to gather your personal information. First, a portable card reader (a device which reads the account information stored in the magnetic strip on the back of your ATM card) will be attached over the ATM machine's own card reader. This portable card reader, or skimmer, is manufactured to look like it is part of the actual ATM. These portable card readers are made not only to read your account information as your bank card is drawn into the ATM machine, but to store it on a memory chip inside the reader.

The next step is to install a small pin hole camera somewhere on the ATM machine which will allow the criminal to view and record you as you enter your personal identification number (PIN number) on the keypad.

After the skimming equipment has been on the ATM machine for several hours, the criminals will remove them and take them to a separate location where your account number information is downloaded from the portable card reader. The video from the camera is then reviewed in order to obtain the PIN numbers which correspond to each account. With this information, the criminals are able to program your account information onto a blank card and then use that cloned card, along with your PIN number, to remove money from your account without your knowledge.

How to protect yourself!

- Look at each ATM or point of sale terminal you use for anything that looks out of place. Although the skimmers are made to look like they belong on the machine, you may find something that looks out of place. Most of the time, the skimmer and camera are attached with double sided tape or glue.
- Pull on the device if it looks out of place.
- Cover up the keypad when you're entering your PIN number to prevent others from learning your private PIN number.
- Check your accounts regularly for fraudulent activity.
- Contact your bank immediately if you discover fraudulent activity on your account.
- Contact the police if you discover fraudulent activity on your accounts or if you observe unusual activity or suspect that a skimming device has been placed on an ATM.